What is Gaggle's procedure for compromised accounts?

Created by Corey Tutewiler
Last updated Jul 18, 2016

An account has been compromised when it has been accessed by someone other than the actual owner. Often, entities will attempt to obtain the login credentials for email accounts in order to send SPAM to email contacts associated with an account.

When Gaggle takes notice of accounts that have been compromised in your school or district, the account is suspended immediately. While the account is suspended, the student will not be able to send or receive mail. The student will still be able to log in to Google or Office 365 and attempt to send messages, but messages will not be delivered.

The school or district main contact will additionally receive an email notification, letting them know that the account was compromised.

When an account is compromised, a Gaggle Administrator at your school or district needs to:

1. Change the account's password in the Google Admin Console or Office 365 Admin Center.
2. Change the account's access level in Gaggle from Suspended back to its original setting.

Here's a link detailing how to change a user's password in Google.

Here's a link detailing how to change a user's password in the Office 365 Admin Center.

To change the access level in Gaggle, follow these steps:

1. Log in to your Gaggle account at https://apps.gaggle.net
2. Select the **Admin** tab, located at the top of the interface.
3. Perform a search for the user you're looking for in the top toolbar and select the user from the search results.
4. After the user's account settings load, locate the **Access Level** field and reset it from **Suspended** back to its original setting.
5. When finished, select the **Save** icon in the top toolbar.

No labels